ISO och LIS

Stefan Jansson

2019-09-02

ISO

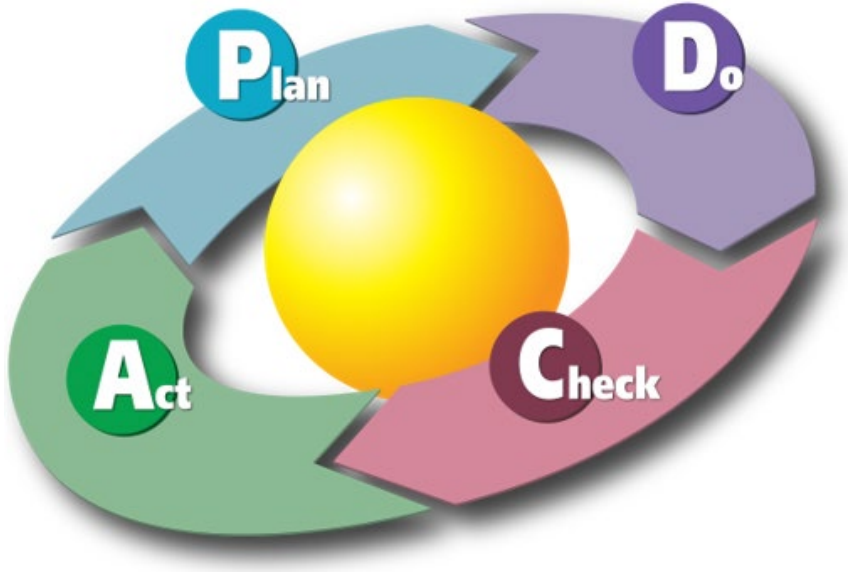
- International Standards Organisation
- Skapad 1947
- Aktiv i 164 länder
- Politiskt och ekonomiskt oberoende
- Över 20 000 standarder

ISO 27000 serien - Informationssäkerhet

- Skapades år 2000
- Baserad på BS 7799 och säkerhetspolicy från Royal Dutch/Shell Group på 80 och 90-talet
- 45 olika standarder

ISO 27001 - Säkerhetsåtgärder

- Har sitt ursprung i BS 7799 från 1995
- Plan – Do – Check – Act
- 114 kontrollåtgärder



ISO 27000 grupper

- A.5: Information security policies (2 controls)
- A.6: Organization of information security (7 controls)
- A.7: Human resource security - 6 controls that are applied before, during, or after employment
- A.8: Asset management (10 controls)
- A.9: Access control (14 controls)
- A.10: Cryptography (2 controls)
- A.11: Physical and environmental security (15 controls)
- A.12: Operations security (14 controls)
- A.13: Communications security (7 controls)
- A.14: System acquisition, development and maintenance (13 controls)
- A.15: Supplier relationships (5 controls)
- A.16: Information security incident management (7 controls)
- A.17: Information security aspects of business continuity management (4 controls)
- A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

Exempel – Säkerhetsåtgärder (MSB)

ID	Beskrivning
2.3.1	Bara godkänd programvara (se rekommendation 1.2.1) bör köras på verksamhetens enheter; använd automatiska verktyg för att förhindra att slutanvändare kör icke-godkända applikationer (vitlistning). Blockera exekverbara filer utanför godkända mappar och på flyttbara media, som till exempel på CD och USB-stickor.
2.3.2	Ändra alla standardlösenord i system och komponenter före produktionssättning. Detta inkluderar t.ex. applikationer, operativsystem, routrar, brandväggar och åtkomstpunkter.
2.3.3	Använd klientbrandvägg som reglerar inkommande trafik och loggar säkerhetsrelevanta händelser

Exempel – Risker (STEM)

	RISK	KONSEKVENS
2.3-R1	En systemkomponent tas i bruk med en oförändrad standardkonfiguration.	Portar lämnas öppna som inte behöver vara öppna.
		Användarprofiler använder lösenord som är kända i branschen och ibland t.o.m. dokumenterade i driftsinformation. Dessa kan användas för att ta sig in i komponenten och sedan in i nätverket.
		En systemkomponent använder äldre och mindre effektiva anti-virus åtgärder.

Krossreferenser till ISO

Beskrivning	ID	ISO
Säkerställ en säker konfiguration av maskin- och programvara	2.3	A.12.5.1
	2.3	A.12.6.2
	2.3	A.14.2.2
	2.3	A.14.2.6
	2.3	A.14.2.7
	2.3	A.14.2.8
	2.3	A.14.2.9

ISO Kontroll

A.12.5 Styrning av driftsystem		
Mål: Att säkerställa riktigheten hos driftsystem.		
A.12.5.1	Installation av program på driftsystem	*Säkerhetsåtgärd* Rutiner ska införas för att styra installation av program på driftsystem.

A.14.2.2	Rutiner för hantering av systemändringar	*Säkerhetsåtgärd* Systemförändringar inom utvecklingscykeln ska styras genom användning av formella riktlinjer för ändringshantering.
		Säkerhetsåtgärd

Energimyndigheten

LIS

- Dokumentation
- Processer
- Ledning - Governance

Hur kommer man igång med LIS?

- Skriv ner det ni redan gör
  - Tekniskt arbete
  - Organisatoriskt arbete
- Policy – Det här vill vi åstadkomma
- Processer – Så här gör vi det
- Granska periodvis

GRC Verktyg

- ”Governance, Risk and Compliance”
- Governance – Styrning
- Compliance - Åtföljning